Prepared Testimony and
Statement for the Record of

Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation

Hearing on:

"Wassenaar: Cybersecurity & Export Control"

Before the

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

and

House Committee on Oversight and Government Reform
Subcommittee on Information Technology

January 12, 2016

2154 Rayburn House Office Building

Chairman Ratcliffe, Chairman Hurd, Ranking Members Kelly and Richmond, and distinguished members of the Committees, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. Currently I serve on the World Economic Forum Global Agenda Council on Cybersecurity, and on the boards of the George Washington University Center for Cyber and Homeland Security, the Information Technology Industry Council, and the National Cyber Security Alliance. From 2010 to 2012 I served as the Chair of the U.S. IT Sector Coordinating Council – one of 16 critical infrastructure sectors identified by the President and the U.S. Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. Previously, I served in various positions at DHS, including as head of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec protects much of the world's information, and is the largest security software company in the world, with 33 years of experience developing computer security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services (Symantec for enterprises and Norton for consumers and small businesses) protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of hundreds of millions of attack sensors recording thousands of events per second, and more than 500 dedicated security engineers and analysts. We maintain nine Security Response Centers and six Security Operations Centers around the globe. Every day we scan 30 percent of the world's enterprise email traffic, and process more than 1.8 billion web requests. All of these resources combined allow us to capture worldwide security data that give our analysts and our security technologies a unique view of the entire Internet threat landscape; which in turn we use to protect our customers' most sensitive data and systems around the world.

Introduction

The hearing you are holding today is extremely timely. It shines a spotlight on a critical issue that threatens the cybersecurity of not only the U.S. technology industry, but also that of all U.S. critical infrastructure companies and organizations that operate or connect to networks overseas. The proposed U.S. cybersecurity export control rule under the Wassenaar Arrangement would severely damage our ability to innovate and develop new cybersecurity products, to conduct real time global research and share information on software vulnerabilities and exploits, and to test and secure global networks and new technology products.

These restrictions would devastate the U.S. cybersecurity industry itself and harm the security of nearly every U.S. multinational company. This rule is not an export control on a few specific tools. It is a stringent new regulation on the entire cybersecurity industry and its customers that would harm the economic and national security of the U.S. Ultimately, it would leave every American less protected against cybercriminals and cyber terrorists.

Industry and academia in the U.S. are at the forefront of designing, testing and developing some of the world's leading cybersecurity technologies. Companies like Symantec rely on unfettered research and communication to innovate and develop the next generation of security technologies. These new regulations would restrict this free-flow of information and impose major new export compliance burdens on all U.S. multinational industries. It would have three significant negative impacts on cybersecurity:

- First, cybersecurity research would be curtailed, as the rule hinders developers and researchers from testing products and networks and sharing technical information about new vulnerabilities and exploits across borders.

- Second, the availability of critical cybersecurity tools would be constrained, as the rule restricts the export of cybersecurity technologies, even to subsidiaries of U.S. companies overseas.
- Third, cybersecurity collaboration and information sharing would be harmed, as the rule deems information to be "exported" once it is shared with non-U.S. persons, even if they physically work for a company here in the U.S.

The significant time and effort that both the government and the private sector have spent jointly searching for a way to redraft the rules has not borne fruit, but not because of a lack of good faith on both sides. The effort has failed because the proposed rule contains unresolvable ambiguities and fundamental flaws – defects that are rooted in the faulty original 2013 Wassenaar cybersecurity agreement. For this reason, the U.S. redrafting effort should be suspended. The U.S. government should take a leadership role and return to Wassenaar in the upcoming plenary session with a proposal to renegotiate the 2013 cybersecurity agreement.

In my testimony today, I will discuss:

- An overview of the Wassenaar Arrangement and the "cybersecurity rule";
- Consequences for cybersecurity tools, testing, research and information sharing;
- Other critical infrastructure sectors affected by the rule;
- Economic impacts of the rule for industry and the government;
- How other Wassenaar nations are implementing the rule; and
- Why the U.S. proposed rule is unworkable, and solutions outside of Wassenaar.

I. Overview of the Wassenaar Arrangement and the "Cybersecurity Rule"

The Wassenaar Arrangement is a multilateral export control agreement with 41 nations as signatories that was established in 1996 and designed to cover conventional arms and dual-use goods and technologies and prevent proliferation of sensitive components.[1] It did not originally envision, nor was it designed for, widely available cybersecurity software technologies. There is a process for adding new controls, and under the 2013 agreement, the United Kingdom offered a proposal that "intrusion" and "surveillance" software be added to the list of export-controlled technologies. This grew out of well-intended concerns over the availability of "intrusion software" to repressive regimes and the need to protect human rights. As the control was being developed, we are not aware of any consultations with the U.S. cybersecurity industry about its real world implications, given that the underlying software functionality of intrusion software is the same or similar to other widely used security technologies.

Though the Wassenaar Arrangement is non-binding, it has long been the policy of the U.S. to fully implement agreements under it and to update its own export control regime accordingly. As part of the U.S. implementation of this new control, in May 2015 the Department of Commerce (DoC) published for comment in the Federal Register a proposed amendment to the U.S. export regulations that would cover cybersecurity products categorized as "intrusion and surveillance items."[2] Due to the overly broad definitions in the Wassenaar control and the subsequent U.S. rule, industry and academia submitted an unprecedented volume of approximately 300 formal comments, nearly all of them strongly objecting to the new regulations.[3]

Symantec, like many others, demonstrated that the rules were written far too broadly and hindered legitimate, widely used and beneficial cybersecurity technologies and practices, including penetration testing

[1] The Wassenaar Arrangement. http://www.wassenaar.org/about-us/.
[2] U.S. Federal Register, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, May 20, 2015. https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items
[3] Department of Commerce Bureau of Industry & Security, see: *Public Comments for Wassenaar Arrangement 2013 Plenary Agreement Implementation*. http://efoia.bis.doc.gov/index.php/electronic-foia/index-of-documents/

software, white-hat research, and cyber threat information sharing.[4] Since the initial comment period, the DoC has proactively engaged in an impressive amount of outreach to solicit advice and input on how they could implement the rule in a way that would not severely damage U.S. economic and national security.

However, the underlying language negotiated at the 2013 Wassenaar Arrangement Plenary was so deeply flawed that, despite months of consultation, we still cannot envision language that would mitigate the numerous detrimental effects. The core problem is that the needed changes do not concern technical definitions or product lists, but instead are an issue of the user's intent when deploying widely available cybersecurity technologies. Unfortunately, the Department of State, as the lead U.S. negotiator at Wassenaar, has repeatedly rebuffed industry concerns on this point, saying the *intent* issue is not up for debate. As such, we see no other alternative than for the U.S. government to return to Wassenaar and renegotiate the underlying and overly broad control that was agreed to in 2013.

It is important to recognize however that Congress understood the importance of this issue from the start, with some of you even submitting your strong concerns through the formal DoC rulemaking process back in July.[5] Moreover, Symantec wishes to thank many of you here today for your leadership in sending a letter last month to the President's National Security Advisor urging the Administration to send the export control rule back to Wassenaar to be renegotiated or heavily revised.[6] Spearheaded by Congressional Cyber Security Caucus Co-chairs Michael McCaul (R-TX) and Jim Langevin (D-RI), the bipartisan letter was signed by 125 Members of Congress and rightly recognizes that the proposed cybersecurity export control regulations will have a chilling effect on research and innovation, as well as negatively impact the overall cybersecurity posture of the U.S.

II. Consequences for Cybersecurity Tools, Testing, Research and Information Sharing

To understand how the proposed rule will harm cybersecurity, it is necessary to understand how common security products and tools work, the technology they are based on, and how the information generated by them is used. Symantec and the larger cybersecurity industry have serious concerns with the ambiguous and overbroad language used in the proposed rule. That language would capture not only cybersecurity products, but also basic software development and security techniques.

Of note, the rule does not specifically control actual "intrusion" software, reportedly so as not to cause victims of cyber hacking whose electronic devices may be carrying intrusion software without their knowledge to commit inadvertent export control violations.[7] Since "intrusion" software is not itself controlled, proponents and the DoC have said the transfer of exploit samples, proofs of concept, and other forms of malware are not controlled. In reality, however, the controlling systems and technology designed to operate, deliver, and communicate with the "intrusion" software effectively sweeps the entire cybersecurity industry – including all penetration testing systems and virtually all other cybersecurity products such as anti-virus software – into the controls.

Unfortunately, it is not possible to effectively share vulnerabilities and exploits for defensive purposes, or to use defensive "intrusion software," without using control and delivery platforms and sharing the equipment, software, and/or technology behind them. While there is ostensibly no direct control of "intrusion software" itself, as a practical matter, the controls are broad enough to effectively control intrusion software by

[4] Regulations.gov, see *Symantec Wassenaar Cyber Rule Comments 07201015*, ID# BIS-2015-0011-0145. http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0145

[5] Regulations.gov, see *Congressional Wassenaar Comments* to RIN 0694-AG49. http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0208

[6] Congressional Letter to Ambassador Susan Rice, December 16, 2015. https://langevin.house.gov/sites/langevin.house.gov/files/documents/12-16-15_Langevin-McCaul_Wassenaar_Letter.pdf

[7] Regulations.gov, see *Wassenaar Arrangement Plenary Agreements Implementation: Intrusion and Surveillance Items*. http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0001

controlling items that generate, operate, deliver or communicate with it, and technology for the development, production, or use of such items. In other words, it is impossible to separate out security software common functionality. Thus, most security technologies end up being swept in for categorical inclusion.

Vulnerability Testing and Patching

Vulnerability testing and patching are examples of how the proposed U.S. rule would put controls on legitimate intrusion software. The DoC has stated that vulnerability scanners, which find potential vulnerabilities in a system without actually exploiting them and extracting data, would not be controlled. But this ignores the reality of the process of vulnerability research, which is not just about finding potential vulnerabilities or even sharing proofs of concept. When finding vulnerabilities and reporting them, the most valuable information is often about how the vulnerability can be exploited and how those exploits work, including the technology used to develop them. This information helps the vendor understand the root cause of the vulnerability and develop a more complete and long-lasting defense instead of just a "band aid" fix. The DoC states that it recognizes that controlled "technology" may be transferred during the reporting of a vulnerability or exploit, highlighting that this process will indeed be subject to these highly restrictive controls. The DoC also recognizes that the tools used to test vulnerabilities (which find vulnerabilities and extract data to prove the vulnerability exists) would also meet the technical description of items that fall within the control list.

Penetration Testing

Controls under the proposed U.S. rule would capture another common and critical set of tools and technology known as penetration testing (often referred to as "pen testing"). Penetration testing is a suite of tests designed to stress the target system (as real attackers would) in its operating environment. It is also used to evaluate the security of a system or software product by analyzing its weaknesses and attempting to compromise it. The testing is best done in a highly controlled environment using specialized computer systems and as part of a broader security testing strategy.

At commercial companies, typically there are two primary categories of penetration testing:

(1) Pre-production penetration testing which is done on products or a family of products before they are released for sale to customers; and

(2) Post-production penetration testing where testers operate on a much broader scope and ensure corporate networks and systems are secure.

In pre-production penetration testing, there are usually three types of tests: black-box, white-box, and gray-box. In a black-box assessment, the testers have no information prior to the start of testing. In a white-box assessment, they will have complete details of the network and applications. For gray-box assessments, the testers will have some details of the target systems. Symantec typically performs gray-box assessments on its own products, as this type of assessment yields more accurate results and provides a more comprehensive test of the security posture of the environment than does a black-box assessment.

In post-production penetration testing, testers take a much broader look into their targeted systems and approach to penetration. This process is, at all times, carefully managed, scoped, and monitored so that any dangerous vulnerabilities discovered are strictly guarded and not allowed outside of the network – or into the "wild". While this testing is directed at the target company's internal networks and systems, often times vulnerabilities in third party hardware and software used in the target's IT environment are also discovered. When these vulnerabilities are discovered, the testers must notify the developer of the vulnerable product and work with them to develop an effective remediation. All data collected, vulnerabilities found, exploits researched and developed, and remediation fixes and approaches are kept strictly within a protected environment for complete safety.

Third Party Software Updates and Patching

Similarly, third parties often engineer "exploits" to provide update services and manual patching for commonly-used software products manufactured by other companies. Such third party participation is necessary to supplement the features offered by the original provider, or where that original provider has gone out of business or has stopped supporting its code, as is often the case with critical infrastructure. Thus, not all exploits are malicious. Unlike auto-updaters that are part of the original software, these third parties use exploits to deliver updates and patches into vulnerable programs and systems. They use these exploits to defeat the integrity of the original system, bypassing its protective measures, modifying its standard execution path, and providing external instructions. Even if the "exploits" themselves are not controlled, the related controls appear to squarely capture parts of these updating and patching tools that deliver and communicate with the components that apply the security patch.

Presumption of Denial for Licenses for Rootkits and Zero-Day Exploits

Another potentially negative impact of the proposed DoC implementation of the rule on the cybersecurity industry and our customers is the rule's presumption of denial for all licenses related to "rootkit" and "zero-day" exploit capabilities.[8] In the preamble to the U.S. proposed rule, in the section titled *License Review Policy for Cybersecurity Items*, it states:

> "Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities."

The presumption of denial for licenses related to rootkit and zero-day exploit functionality is highly problematic. First, the policy would limit the development and delivery of defenses for the most dangerous vulnerabilities, zero-days. Zero-day vulnerabilities are previously unknown and unpatched vulnerabilities and make up the majority of what is discovered during penetration testing. In fact, many cybersecurity companies have zero-day focus groups, which specifically research these types of vulnerabilities and proactively exchange information about their exploitability with other vendors and/or manufacturers to help devise an effective defense. If zero-days are defined as vulnerabilities without a released patch, then they are the highest priority items for responsible companies to address, and it would be highly problematic if they were restricted from being shared with knowledgeable employees or outside experts, some of whom will inevitably be foreign nationals. If a company is prevented from closing a known vulnerability, the security of its customers and its own networks and products will be put at much greater risk, as cyber criminals are quick to act on these.

The presumptive denial for rootkits is similarly problematic. While the functionality of "rootkits" may vary and the term can mean different things in different contexts, a "rootkit" capability is often understood to mean simply that the item can live underneath the user interface and subvert what the user is doing without his or her knowledge. Basically, the rootkit subverts part of the operating system by interrupting it, running "underneath" it, or "hooking" into it. Then, when the operator of the system takes an action, the "rootkit" intercepts that action and modifies or subverts it without the user's knowledge so that it acts differently than as intended.

If this common definition is how the DoC interprets "rootkit" capability in the proposed rule (which is unclear since no definition is provided), any software security instrumentation framework could be seen to create a rootkit capability. Modern security modules often use "rootkit-like" functionality to integrate into the existing code of the operating system; and in doing so change the behavior of the operating system. This is known as "hooking into" an operating system. As such, a fundamental part of most security vendors' endpoint protection products are "rootkit" capabilities. For instance, when you install Symantec's Enterprise or Norton security products, they often work by hooking into the normal operating system, monitoring the data

[8] Regulations.gov, see *License Review Policy for Cybersecurity Items*.http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0001

communicated through it, intercepting and inspecting the data, and potentially changing it when it identifies a threat—all operating in the background once installed on a device. These "rootkit" capabilities are used in these products because they are the most effective means of accessing the system to monitor for and catch malicious traffic before it can fully infect the system.

"Rootkit" capabilities also are a common function of legitimate software, not just for cybersecurity. Examples include remote control software used by help desk technicians, system administration tools, technical support, and even anti-cheat mechanisms for video games. These types of software programs with "rootkit capabilities" are not malicious, but the proposed rule does not distinguish between those used with a system administrator's or user's knowledge, and those put there by a malicious actor. In light of the broad range of legitimate uses for "rootkit" capabilities, a policy of presumptive denial is clearly inappropriate and does not account for how security software is designed for interoperability.

Simply put, not every rootkit or zero-day is shared or used for malicious purposes – the cybersecurity industry uses these same "exploits" in order to fix dangerous vulnerabilities. Indeed, these zero-day vulnerabilities and exploits are the very items that companies seek to find and deal with in their penetration testing engagements and exercises. The inability to freely share this information and the related research and development of defenses within a company and its suppliers will severely impact the ability to create safe products and ensure a secure network and IT environment.

Further, the proposed rule will do nothing to curtail the underground market where criminals buy and sell exploits, vulnerabilities, and attack kits. What it will do is make it harder for U.S.-based organizations with operations around the world to deploy the best tools available to find the weaknesses in their own systems and to patch them – before an attacker does.

Real-Time Information Sharing

The cyber threats we face every day are growing in both numbers and sophistication. Over the last three years we have seen more than *one billion* identities exposed through breaches. Sensitive trade secrets and intellectual property are being pilfered at an unprecedented rate. As detailed in Symantec's 2015 Internet Security Threat Report (ISTR), the use of malware is growing and becoming more sophisticated, with nearly *one million* new variants released every day.[9] Attackers are constantly evolving and honing their capabilities to avoid detection, and there are a broad set of tools available to them.

Vulnerabilities continue to be a big part of the security picture, where operating system and other patches have been critical to helping keep systems secure. For example, in April 2014, the discovery of the *Heartbleed* vulnerability, and its widespread prevalence exposed millions of consumers and businesses worldwide to attack.[10] This vulnerability existed in the underlying web authentication protocols (SSL and TLS) and given the seriousness, created a global call to action for companies, researchers and governments. Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a massive surge of attacks, and cybersecurity professionals around the world mobilized to coordinate and respond.

This is the exact type of urgent and necessary global collaboration that would be impractical and severely hindered under the U.S. rule where we would be required to apply for and wait for an export license before discussing such vulnerabilities with non-U.S. nationals. Compounding the issue is that even if all parties applied for an export license to be able to share such information, that request would be presumptively denied under the proposed U.S. rule.

[9] Symantec ISTR, April 2015. http://www.symantec.com/security_response/publications/threatreport.jsp
[10] Symantec Security Response, *Heartbleed Bug Poses Serious Threat to Unpatched Servers*, April 9, 2014. http://www.symantec.com/connect/blogs/heartbleed-bug-poses-serious-threat-unpatched-servers

Another area that would be impacted is information sharing with global law enforcement and government agencies. Today, Symantec shares cyber threat information with international cyber response organizations and law enforcement entities around the world, including INTERPOL, EUROPOL, and national CERTs and cyber police agencies. This work often extends to specific global cybercrime cases, such as botnet eradication and criminal prosecutions.

For example, in February of 2015, Symantec and other industry players partnered with EUROPOL and other international law enforcement agencies in an operation to disable the infrastructure controlling the *Ramnit* botnet and the criminal gang that operated it.[11] *Ramnit* harvested banking credentials from its victims and had infected more than 3.2 million computers across the globe. It is a fact that cybercriminals do not recognize national borders when they commit crimes. However, under the U.S. proposed rule, Symantec could be required to seek a license every time we wanted to share threat information across borders with international law enforcement, severely limiting the successful public-private partnerships to date.

Further, as a global cybersecurity company, Symantec has researchers, engineers and analysts in our operations centers around the world. Under the current U.S. rule, our American employees working in the U.S. would be required to first obtain a government license if they were going to engage in anything more than a cursory conversation about new security vulnerabilities or exploits with any co-worker who is either not a U.S. citizen or who is located outside the U.S. (even if that foreign-based employee was a U.S. citizen). Further, if our U.S. researchers discovered a zero-day vulnerability in one of our non-U.S. customer's products or systems, and we wanted to share that information with the customer, again we would be required to obtain an export license.

In addition, the rule does not envision the accommodation of real-time machine-to-machine information sharing across borders – a function that modern security analytics, detection and protections heavily rely on today. At a time when cyber threats are increasing, it is critical that sharing of cyber threat information – whether by humans or machines – remains unfettered. Long a priority for the Congress and the Administration and as seen in the recently enacted law, cyber threat information sharing would suffer under this export control.

The simple fact is that the rule will do little to stop the spread of malicious intrusion and surveillance tools, or curtail illicit hacking and intrusions in any way. In fact, the current rule would do just the opposite – handcuff security vendors and multinational companies from using all the tools available to them, while imposing no restrictions on cyber criminals.

III. Other Critical Infrastructure Sectors Affected by the Rule

The proposed rule would have severe impacts beyond just the cybersecurity industry as other critical infrastructure sectors and academia would also be required to obtain export licenses for the use and deployment of these tools. Certain industries are legally required to conduct penetration testing, and some have implemented this type of testing as part of their industry standards and best practices, including the financial services, electricity, and healthcare industries.

Under the proposed rule, companies using testing tools on their networks or facilities outside of the U.S. in order to comply with regulatory requirements and industry standards also will need to implement costly and time-consuming changes to their internal compliance programs to obtain export licenses. The consequences of the delays created will undermine existing industry standards and regulations, weaken security, and lead to more frequent security breaches across critical infrastructure sectors.

[11] Symantec Security Response, *Ramnit cybercrime group hit by major law enforcement operation*, February 25, 2015. http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation

The financial services industry has its own unique information security requirements. A frequent target of attacks, banks perform a high level of due diligence to ensure the confidentiality, integrity and availability of customer transactions. Penetration testing is one way to stress the attack surface that an organization presents to the outside world. Under the rule, any multinational U.S. financial institution would be required to seek export licenses before testing its own global networks. As the Financial Services Roundtable/BITS made clear in its formal comments to the DoC, the proposed rule would "seriously diminish the financial industry's ability to effectively run day-to-day cybersecurity assurance programs."[12]

The power industry is another critical infrastructure sector that is required to conduct penetration testing. As part of the North American Electric Reliability Corporation (NERC) CIP standards (007-011), cybersecurity testing is recognized as a critical factor in protecting the nation's electric grid. In addition, the National Electric Sector Cyber Security Organization Resource (NESCOR) has created a security test plan template to provide guidance to electric utilities on how to perform penetration tests on Smart Grid systems.[13] Similarly, the healthcare industry has heightened privacy and security concerns associated with the electronic transmission of health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 strengthened civil and criminal penalties for breaches and non-compliance with HIPAA standards. By restricting the necessary cybersecurity tools to test overseas networks and products, the rule will make compliance with such requirements more difficult for U.S. multinational companies.[14]

Information sharing would also be an issue for the critical infrastructure sectors. The Financial Services ISAC and the Energy ISAC, both with successful information sharing programs among their company members, also would likely be required to obtain export licenses in order to conduct their business across borders. In addition, in the healthcare sector, one could imagine a scenario where a U.S. multinational healthcare device manufacturer discovers a life-critical, zero-day vulnerability in a product. Under the U.S. rule, the company would be prohibited from sharing details with its experts – or even its customers – around the world while it waits for weeks or months to obtain an export license. Meanwhile, the vulnerability would sit unfixed and open for attack during that time.

IV. Economic Impacts for Industry and Government

U.S. companies design, test and deploy much of the world's leading security technology. The U.S. is also home to most of the world's cybersecurity companies, holding the number one provider position in the global market – which topped $75 billion in 2015 and could reach $170 billion by 2020.[15] The proposed rule will have a disproportionate effect on the U.S. cybersecurity industry, because most of the companies are based here. In addition to the economic effects on the cybersecurity industry, the rule would also lead to less secure networks and make them easier prey for cybercriminals. While estimates vary, cybercrime experts have put the annual global cost of cybercrime at $400 billion or more.[16] Without the benefit of cutting edge research and security available to consumers and companies, this number could rise significantly.

Companies implementing the new rule will surely feel the financial impacts as significant new legal and compliance resources will be needed just to manage this one regulation. At Symantec, our preliminary

---

[12] Regulations.gov, Financial Services Roundtable/BITS comments. http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0231

[13] NESCOR, *Guide to Penetration Testing for Electric Utilities - Version 3*, 2013. http://smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf

[14] Regulations.gov, Coalition for Responsible Cybersecurity comments. http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0209

[15] Morgan, Steve. *Worldwide cybersecurity market continues its upward trend*, CSO Online, July 9, 2015. http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-and-projections.html

[16] Center for Strategic & International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014. http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

assessment showed that initially we would need approximately one thousand new licenses, but the actual number could go much higher. This is in comparison to our current annual filings that number less than a dozen. Equally as important, the new regulations would require us to significantly alter our trade compliance program. These changes would result in the hiring of additional compliance personnel and a six-month lead time to collect the information necessary to submit any new export license requests. The added burdens would impede Symantec's ability to be nimble and agile in responding to real-time threats and cyber attacks.

Further, it is not clear how we would even write a license application given the fact that our penetration testing processes allow for detection of unanticipated vulnerabilities and additional follow-on testing if needed. We envision a scenario where we conduct a test, find that we need to do more or different testing, and then must stop to wait weeks or months for another export license. In the meantime, our networks could remain vulnerable, or our product development and security protection release cycles would be significantly delayed. Both of these would have substantial financial and market impacts on our business. We envisage that most other companies would incur similar economic impacts.

There are also implications for cybersecurity start-ups and small businesses who do not have the compliance programs that large companies have, or know how to deal with these rules. By placing such a heavy compliance burden on small innovators, the likely end result is that the U.S. will drive the cybersecurity industry offshore as the U.S. system will be too complex and resource intensive. When combined with a more stringent U.S. implementation than other nations, start-ups will be even more competitively disadvantaged.

On the government side, the proposed rule represents an unknown but significant licensing burden for the DoC Bureau of Industry and Security (BIS) that is responsible for managing the U.S. export control regime. The exponential increase in license applications from all industries, coupled with the enforcement needed to ensure compliance, would require significant new taxpayer resources. It is highly unlikely that the BIS, as is currently staffed, has the capacity to evaluate and process such a large volume of new applications.

V. International Implementation

Not only do the proposed Wassenaar controls damage U.S. economic and national security, but they also do not effectively control the very export of the items they are targeting. For one thing, countries that are party to the Wassenaar Arrangement and who already implemented the rule have taken vastly different approaches. There are multiple interpretations of the underlying Wassenaar agreement language that have led to confusion and implementation that differs significantly from country to country. It is clear that the requirements under the Wassenaar Arrangement differ significantly from how countries are implementing the rule.

For example, in Japan, the government worked closely with industry and the Center for Information on Security Trade Controls, resulting in broad carve-outs for nearly any conceivable cyber security product, technology, and research. However, in the end and when viewed clearly, this is simply a case where a Wassenaar country has recognized that there is no way to control malicious hacking products and technology without also causing severe damage to the legitimate cybersecurity industry and its customers. Unintentionally, Japan has added to the variations on implementation of the control, which inevitability will hold up multinational companies' testing and development work.

A direct result of this ambiguity occurred in 2015 when Hewlett-Packard (HP) and its Zero Day Initiative declined to participate in an annual hacking contest in Japan. HP's head of threat research, Jewel Timpe, cited Japan's implementation of Wassenaar as the reason, and that the risk associated with the real time transfer of research across borders could not be reconciled by their legal and compliance teams. She said, "It's due to difficulty in handling, defining and getting the licensing in real time that the contest demands. On the ground running the contest, how does one effect transfers and not run afoul of the arrangement? There was no clear

path to do that easily and quickly."[17] There is no doubt that the same questions and lack of clarity will stifle and impede critical research, sharing, and innovation for the legitimate cybersecurity industry across all of the countries that implement the rule.

In the case of Italy, their implementation is essentially in name only with little to no enforcement mechanism in place. Take for example the Hacking Team, a Milan-based information technology company. The Hacking Team's public business model was to sell offensive intrusion and surveillance capabilities – the exact technology the Wassenaar Arrangement attempted to target with the new controls. However, the Italian export authorities granted a blanket global license to the Hacking Team allowing them to freely export their products around the world to many of the countries that the Wassenaar rule is trying to prevent from obtaining these tools.

Some companies who make products originally targeted to be controlled under the Wassenaar rule simply move to different jurisdictions to avoid onerous or explicit export controls on their products. The Gamma Group, owner of FinFisher (a type of surveillance software known as spyware) has opened subsidiaries and closed others in a number of European countries and the British Virgin Islands, at least in part to what appears to be to avoid export controls. Indeed today, the legal status of the FinFisher product appears to be held by a completely separate entity from Gamma. Yet, they were still seen exhibiting their products at an arms fair in Paris recently.

The signatories to Wassenaar represent roughly 25 percent of the countries in the world. The group excludes many countries with growing cybersecurity industries and capabilities, such as Israel and China. Even if the rule were to be implemented uniformly, 75 percent of the world would not be bound by these regulations, putting those who rigorously implement and enforce the rule at a distinct competitive disadvantage. Moreover, the rule would not have its desired effect because the countries that have been accused of using malicious exploits for espionage or using surveillance software to spy on dissidents will still be able to obtain the controlled technologies from other markets. These technologies are already widespread and ubiquitous, and in many cases they are free on the Internet, so as to be nearly impossible to control.

During extensive international outreach and education regarding the impacts of the Wassenaar rule, some officials in European Union (EU) member nations have expressed a recognition that they may have overreached with the original Wassenaar control. Some have indicated a willingness to revisit the control and explore possible fixes at the upcoming Wassenaar Plenary. Indeed, many technical experts and EU export regulators have expressed concern that controls with no technical parameters or thresholds – such as the intrusion and surveillance software rules – will ultimately undermine the overall intent of the Wassenaar Arrangement if not addressed and corrected.

VI. Attempts to Re-write the Proposed U.S. Rule are Unworkable

As evidenced by the approximately 300 formal comments to the proposed rule, and as discussed in my testimony, a number of serious technical issues have been raised concerning these controls. Due to these technical complexities, the DoC released two additional FAQ documents to try to explain what was and was not covered under the proposed rule.[18] However, to its credit, the DoC recognized the validity of these concerns and quickly withdrew the proposed rule in July.[19] In the weeks and months since, industry and government have met multiple times seeking a common understanding of the issues with the rule, and possible ways to redraft it. The conversations that followed were extensive and frank – and ultimately

[17] Mimoso, Michael. *Citing Wassenaar, HP Pulls Out of Mobile Pwn2Own*, ThreatPost, September 4, 2015. https://threatpost.com/citing-wassenaar-hp-pulls-out-of-mobile-pwn2own/114542/

[18] Regulations.gov, FAQs, June 18, 2015 and July 13, 2015. http://www.regulations.gov/#!docketBrowser;rpp=25;po=0;dct=SR%252BO;D=BIS-2015-0011

[19] Mimoso, Michael. *Unusual Re-Do of US Wassenaar Rules Applauded*, ThreatPost, July 31, 2015. https://threatpost.com/unusual-re-do-of-us-wassenaar-rules-applauded/114096/

unsuccessful. They failed for a simple, inescapable reason – the 2013 underlying Wassenaar controls are fundamentally flawed.

There have been no suggestions for technical fixes to the language used in these controls because the issues with the rule are not technical. The core problem remains one of "intent"; fixes to technical definitions or product lists will not solve this issue. All multinational companies need to employ tools for computers or networks that have the functional specifications of the control parameters to avoid detection, defeat protective countermeasures, extract data or information, modify system or user data, and modify the standard execution part of a program or process to execute externally provided instructions. These are the exact hallmarks a malicious attacker's software would have and what an assessment team would hope to replicate. Thus, the issue becomes one of user intent.

Industry's concern, then, with the existence of such a rule is that it is not possible to use a technical description of the "malicious" tools used by malicious actors to distinguish them from the "legitimate" tools used by the cybersecurity industry – they are effectively the same tools – in an attempt to revise or carve-out exceptions that would allow legitimate cybersecurity uses. Therefore, the rule is both over-broad and will be ineffective in that it does not target that which the drafters presumably intended to target – those with malicious intent.

In addition, the use of exceptions by member states to enable a reasonable implementation of the controls leads to fatally flawed inconsistencies across the Wassenaar members. These inconsistencies lead to continuing questions by multinational companies regarding what is, and is not, controlled – creating a significant compliance burden. Moreover, the U.S. implementation creates competitive disadvantages for U.S. companies who are held to a completely different standard than the rest of the member states.

It has proven to be very difficult, if not impossible to develop fair and consistent exceptions allowing unfettered transfers of such things as generic tools, not designed for purposes of "intrusion", which can also be used to generate, operate, deliver, or communicate with intrusion software. In order to hide from defenders, many new malware packages rely on existing features of complex operating systems to compromise devices and networks. While authorized teams use tools that would be controlled under Wassenaar, the malicious attackers would freely obtain the tools they need from non-commercial hacking sites. More advanced attackers and state-sponsored hackers would even develop their own custom tools – all while the legitimate users who need to develop the tools or use them for protection are limited from obtaining them while they wait weeks or months for their export licenses.

Altering the controls by developing carve-outs and exceptions are impossible to develop, enforce, and consistently apply. Limited exceptions other than defaulting to end use controls would render the controls ineffective. Realistically, the spread of these tools and technology cannot be limited when most if not all of the tools and technology are already available to non-member countries and large non-state criminal organizations. We believe creating carve-outs and exceptions will ultimately stifle innovation into new areas and techniques for cyber security defense, which cannot be predicted.

At the same time, any such list of exceptions would itself quickly become outdated as new cyber security products that do not match these descriptions are developed. And as noted above, any list of exceptions would be inconsistently applied across the Wassenaar states, thus creating uncertainty for multinational entities as to when a control applies and when it does not. Perhaps a better question to ask is whether the Wassenaar export control regime, or any export control regime, is the right approach to use in controlling the spread of malicious hacking tools and technology?

VII. Solutions Outside of the Wassenaar Arrangement Construct

As discussed throughout this testimony, Symantec believes that revising the proposed U.S. rule will not mitigate the negative effects of the original Wassenaar controls. However, there are more effective ways to address the problematic activity that the rule was designed to deter.

For example, the malicious cyber activity that is targeted under this rule could be countered under criminal law statutes that exist today. The U.S. government could dedicate additional resources to the FBI and federal prosecutors. Over the last decade the FBI and the Department of Justice have developed substantial experience in cyber investigations, forensics, and prosecutions. An export control regime managed by the DoC does not achieve these goals, especially since the technology will still be widely available throughout the world. Malicious cyber attacks are often based overseas, working with abusive foreign governments or underground criminal networks, which are threats that the DoC is neither resourced nor well-suited to address. Ultimately we go back to the fundamental flaw in the proposal – that technology-based export controls are the wrong mechanism to address cybercrime. Controls that are more capable of targeting the ill intent of the people using the software or technology are more suited for this purpose.

Sanctions are another tool that the U.S. government can use to address this threat. The Treasury Department's Office of Foreign Assets Control (OFAC) is already experienced and heavily engaged in this area. On April 1, 2015, the President issued Executive Order (EO) 13694 titled: *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.* Its purpose is to "enable the U.S. government to block the property and assets of extraterritorial actors involved in cyber attacks, who have otherwise been difficult to reach."[20] These cyber-enabled activities occurring outside the U.S. may constitute a significant threat to the "national security, foreign policy, or economic health or financial stability of the U.S." The Treasury Department's OFAC could dedicate more resources to carry out the EO and serve as a stronger global deterrent to malicious cyber actors. While OFAC just issued regulations implementing the EO last week, to date no designations have been issued.[21]

Conclusion

Since the U.S. cybersecurity export regulation was proposed in May of 2015, Symantec – together with a broader coalition of the cybersecurity industry and from across the critical infrastructure sectors – has engaged with the Administration about the significant negative consequences and dangers that this new export control regime will bring.[22] While many in the Administration have been receptive to our concerns, including the DoC and DHS, others have held steadfast to a position that ignores the realities of today's global cybersecurity ecosystem.

As described throughout my testimony, to implement the proposed U.S. regulation, or any variation of the underlying Wassenaar cyber rule, would have catastrophic effects on the cybersecurity industry, multinational corporations that rely on these technologies, and U.S. economic and national security. Any controls in this area should be focused on the intended use, rather than this widely-used technology upon which the world depends. The U.S. government should seek to utilize other authorities and mechanisms as described above to address this issue.

At a time when global cyber threats are increasing every day, it is imperative that the private sector and academia be able to conduct research and provide citizens, businesses, and governments with cutting-edge security products to keep pace with the growing threat. This is no time to restrict the availability of security tools and our ability to share information for cybersecurity purposes.

Symantec strongly recommends that the rule be remanded back to Wassenaar to be renegotiated and more narrowly defined. We look forward to continuing to work with the U.S. government and sharing our technical expertise to achieve an outcome that benefits cybersecurity in the U.S. and around the world.

[20] Perkins Coie, *President Issues Executive Order to Block Assets of Foreign Cyber Attackers,* April, 2015. http://www.jdsupra.com/legalnews/president-issues-executive-order-to-bloc-76757/

[21] Steptoe & Johnson, LLP, *OFAC Issues Cyber-Related Sanctions Regulations*, January 7, 2016. http://www.steptoe.com/publications-10990.html

[22] Coalition for Responsible Cybersecurity. http://www.responsiblecybersecurity.org.